

REMARKS

Claims 175-181, 184-188, 190-198, 201-205, 207-215, 218-222, 224 and 225 are pending, of which claims 175, 192 and 209 are in independent form.

Claims 175, 192 and 209 are amended by the present response. Support for the amendments may be found in the published patent application, for example, at Paragraph [0147], *inter alia*.

Favorable reconsideration of the present patent application as currently constituted is respectfully requested.

Regarding Priority

The Examiner states that the claims of the present application are not entitled to an effective filing date of the priority documents. Applicant continues to maintain that under MPEP §201.08, a Continuation-in-Part (CIP) application should be permitted to claim the benefit of the filing date of an earlier non-provisional application if the CIP application otherwise complies with 35 U.S.C. §120 and 37 C.F.R. §1.78. Applicant reserves the right to perfect any priority claim as may be deemed appropriate.

Regarding the Claim Rejections - 35 U.S.C. §103

Part I

In the pending Office Action, claims 175, 178, 179-181, 184-188, 190, 192, 195-198, 201-205, 207, 209, 212-215, 218-222 and 224 stand rejected under 35 U.S.C. §103(a) as being unpatentable over "AirMobile Software of Lotus cc:Mail Wireless: Communication Server Guide" (hereinafter the *AirMobile* reference) in view of U.S. Patent No 6,807,277 to Doonan et al. (hereinafter the *Doonan* reference).

In connection with these rejections, the Examiner has commented as follows with respect to base claim 175:

... While AirMobile teaches the use of a "secure and authenticated" channel (p. 25), it fails to specifically disclose that encrypting the messages prior to transmitting them via the channel using encryption/ decryption keys sent to the redirector host and mobile device (via a secure connection) by the computer system associated with the user.

Doonan discloses a similar system for transmitting electronic messages (Abstract). Doonan teaches use of a key server that sends encryption keys to message "senders" and decryption keys to message "recipients" (col. 3, ll. 33-58, wherein the keys may be sent via secure connections (secure HPPT)(col. 3, ll. 40-42). Doonan discloses that the "senders" and "recipients" may be computers associated with users or software programs operating in an unattended "server mode" (col. 3, ll. 18-31). The addition of a key server to AirMobile's system would have been advantageous since it would have provided encryption keys to the redirector host, decryption keys to other mobile device, and allowed messages to be encrypted to protect

the messages from interception during transmission to the mobile device.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the redirected messages prior to transmission to ensure that they were not intercepted by unauthorized recipients during transmission to the client.

Applicant respectfully submits that the pending §103(a) rejections as set forth above have been overcome or otherwise rendered moot by way of the present amendment.

As defined by base claim 175, an embodiment of the present disclosure is directed to a method of redirecting data items from a messaging host system to a user's mobile device. The method comprises, *inter alia*, sending a first encryption key, which is generated at the computer system associated with the user in dependence on the user's interaction therewith, to the redirector host system and storing the first encryption key at the redirector host system. The method further comprises the redirector host system detecting a new data item for the user at the messaging host system and determining whether the new data item should be redirected to the user's mobile device. If the new data item should be redirected, the method comprises encrypting the new data item to form an encrypted new data item using a cipher algorithm and the first encryption key at the

redirector host system and transmitting the encrypted new data item from the redirector host system to the user's mobile device.

Additionally, base claim 192 and base claim 209 contain substantially similar features.

The *AirMobile* reference is directed to forwarding a user's email to a mobile device. As the Examiner has acknowledged, *AirMobile* fails to teach encrypting the messages prior to transmitting them. *AirMobile*, therefore does not anticipate or suggest sending a first encryption key, which is generated at a computer system associated with the user in dependence on the user's interaction therewith, to the redirector host system, as is now recited in claim 175.

Doonan is directed to a secure messaging system that utilizes a key server. As *Doonan* discloses with reference to FIG. 2, reproduced herein for convenience, whenever sender 100 wants to send an

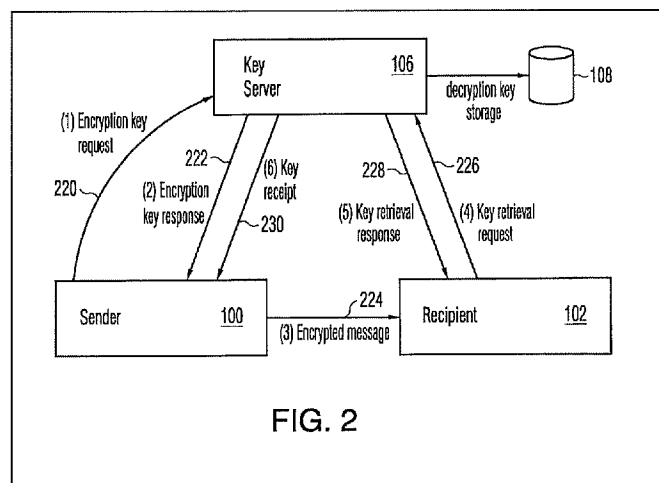


FIG. 2

encrypted message, sender 100 sends a request (220) for a key to key server 106, which returns (222) an encryption key to sender 100 and makes a decryption key available on request to recipient

102. *Doonan* does not, however, disclose that the encryption key is generated at a computer system associated with the user. *Doonan's* key server is not a computer associated with the user, so the key is not generated at a computer associated with the user. Additionally, *Doonan's* key server does not create an encryption key in dependence on the user's interaction therewith. Applicant submits that even if the key server of *Doonan* were incorporated into the system of *AirMobile*, as the Examiner has proposed, the combination does not meet the limitation that the encryption key that is sent to the redirector system is generated at the computer associated with the user in dependence on the user's interaction therewith.

Based on the foregoing, Applicant respectfully submits that the base claims 175, 192 and 209 are not anticipated or suggested by the applied art of record, and are therefore in condition for allowance. Claims 178-181, 184-188, 190, 192, 195-198, 201-205, 207, 209, 212-215, 218-222 and 224 each depend from one of base claims 175, 192 and 209 and introduce additional limitations therein. Accordingly, these dependent claims are also believed to be in condition for allowance.

Part II

Claims 177, 194 and 211 are rejected under 35 U.S.C. §103(a) as being unpatentable over *AirMobile* in view of *Doonan* and U.S. Patent Application Publication No. 2005/0278641 to Mansour et al. (hereinafter the *Mansour* reference).

Claims 191, 208 and 225 are rejected under 35 U.S.C. §103(a) as being unpatentable over *AirMobile* in view of *Doonan* and ARDIS ("ARDIS Begins Shipping New Lan-Based E-Mail Software; First Wireless Data Network to Offer Solution for Microsoft Mail and Lotusr (sic) cc:Mail Applications; Supports New Motorola Envoy 150 Wireless Communicator") (hereinafter the *ARDIS* reference).

Applicant respectfully submits that the pending §103(a) rejections as set forth above have been overcome or otherwise rendered moot by way of the present amendment.

The Examiner has admitted that *AirMobile* does not disclose encryption and does not disclose the use of encryption keys. As noted in the earlier arguments, *Doonan's* key server is not a computer associated with the user, so the key is not generated at a computer associated with the user. Additionally, *Doonan's* key server does not create an encryption key in dependence on the user's interaction therewith.

The additional references, i.e., *Mansour* and *ARDIS* do not cure the deficiencies of the *AirMobile* and *Doonan* references. *Mansour* is directed to a Java calendar application delivered to a web browser. *Mansour* notes that encryption is an important feature, but does not disclose any details of the encryption process. The *ARDIS* reference is an announcement of electronic mail software that supports Apple® MessagePad. Neither of these references discloses or suggests sending a first encryption key from a computer system associated with the user to a redirector host system.

Based on the foregoing, Applicant respectfully submits that claims 177, 191, 194, 208, 211 and 225 are also believed to be in condition for allowance.

Reservation of Rights

Notwithstanding the foregoing, Applicant reserves all rights not exercised in connection with this response, such as, e.g., the right to challenge or rebut any tacit or explicit characterization of any reference or of the present claims, the right to challenge any Official Notice(s) taken, the right to challenge or rebut any asserted factual or legal basis of any of the rejections of the present Office Action, or the right to swear behind any cited reference such as provided under 37 C.F.R. §1.131 or otherwise.

Fee Statement

Compared to the highest number previously paid for, the total number of claims and the number of independent claims have not increased. No extension of the response period is being sought. Accordingly, Applicant believes no fees are due for the filing of this response. If any additional fees are due and/or any overpayments have been made, however, please charge and/or credit our deposit account (Deposit Account No. 03-1130).

SUMMARY AND CONCLUSION

In view of the fact that none of the art of the record, whether considered alone or in combination discloses, anticipates or suggests the presently pending claims and in further view of the above amendments as proposed and remarks, reconsideration of the Action and allowance of the present patent application are respectfully requested and are believed to be appropriate.

Respectfully submitted,

Dated: February 26, 2009

/Betty Formby/
Betty Formby
Registration No. 36,536

THE DANAMRAJ LAW GROUP, P.C.
Premier Place, Suite 1450
5910 North Central Expressway
Dallas, Texas 75206
Tel (214) 750-5666
Fax (214) 363-8177